

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

TREVOR SLOAN, JOSEPH BLEIBERG,
ARYEH LOUIS ROTHBERGER, KEVIN
FARR, ELMER ORPILLA, and SAGAR
DESAI, on behalf of themselves and all
others similarly situated,

Plaintiffs,

vs.

ANKER INNOVATIONS LIMITED,
FANTASIA TRADING LLC, and POWER
MOBILE LIFE LLC,

Defendants.

Case No. 1:22-cv-07174

Honorable Sara L. Ellis

**DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF
OPPOSED MOTION FOR JUDGMENT ON THE PLEADINGS**

TABLE OF CONTENTS

	Page
INTRODUCTION	1
RELEVANT FACTUAL ALLEGATIONS	2
LEGAL STANDARD.....	5
ARGUMENT	5
CONCLUSION.....	9

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Adams v. City of Indianapolis</i> , 742 F.3d 720 (7th Cir. 2014)	5
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	5
<i>Avery v. State Farm Mut. Auto. Ins. Co.</i> , 835 N.E.2d 801 (Ill. 2005)	5
<i>Barnett v. Apple Inc.</i> , 225 N.E.3d 602, (Ill. 2022)	3, 8
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	5
<i>Campana v. Nuance Commc'ns, Inc.</i> , No. 21 CV 1241, 2024 WL 2809838 (N.D. Ill. Mar. 8, 2024)	passim
<i>G.T. v. Samsung Elecs. Am. Inc.</i> , 742 F. Supp. 3d 788 (N.D. Ill. 2024)	8
<i>Gladstone v. Amazon Web Servs., Inc.</i> , 739 F. Supp. 3d 846 (W.D. Wash. 2024).....	4
<i>Mayhall on behalf of D.M. v. Amazon Web Servs. Inc.</i> , No. C21-1473-TL-MLP, 2022 WL 2718091 (W.D. Wash. May 24, 2022).....	4
<i>McGoveran v. Amazon Web Servs., Inc.</i> , No. 1:20-CV-01399-SB, 2024 WL 4626253 (D. Del. Oct. 30, 2024).....	passim
<i>Monroy v. Shutterfly, Inc.</i> , No. 16 C 10984, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017).....	5
<i>Mussat v. Power Liens, LLC</i> , No. 13-CV-7853, 2014 WL 3610991 (N.D. Ill. July 21, 2014).....	4
<i>Stein v. Clarifai, Inc.</i> , 526 F. Supp. 3d 339 (N.D. Ill. 2021)	6
<i>Vance v. Google LLC</i> , No. 20-CV-04696-BLF, 2024 WL 1141007 (N.D. Cal. Mar. 15, 2024).....	passim

Statutes

740 Ill. Comp. Stat. 14/1 *et seq.*.....1

Fed. R. Civ. P.12(b)(6).....5

Fed. R. Civ. P. 12(c)5

Other Authorities

AWS, Global Infrastructure, Regions and Availability Zones,
https://aws.amazon.com/about-aws/global-infrastructure/regions_az/ (last
visited February 18, 2025)4

INTRODUCTION

On June 6, 2023, Defendants Anker Innovations Limited (“Anker”), Fantasia Trading LLC (“Fantasia”), and Power Mobile Life LLC (“Power Mobile Life”) (collectively, “Defendants”) filed a Motion to Dismiss arguing that certain Plaintiffs could not maintain a claim under the Biometric Information Privacy Act (“BIPA”), 740 Ill. Comp. Stat. 14/1 *et seq.*, on behalf of non-Illinois residents, because BIPA applies only to conduct that “occur[s] primarily and substantially in Illinois.” Mot. to Dismiss at 14, ECF No. 45-1.¹ On January 9, 2024, this Court “agree[d],” holding, for that very reason, “BIPA does not apply to the non-Illinois residents,” and dismissing the BIPA claim as to non-Illinois Plaintiffs accordingly. Op. & Order at 12–13, ECF No. 66.

Since then, the caselaw applying BIPA has evolved, and now makes clear that even Illinois-resident plaintiffs cannot maintain a BIPA claim unless they allege facts showing the defendant’s “collecting and storing [of] the biometric information . . . occurred in Illinois.” *Campana v. Nuance Commc’ns, Inc.*, No. 21 CV 1241, 2024 WL 2809838, at *3 (N.D. Ill. Mar. 8, 2024). What is more, this same caselaw explains that it does not suffice to allege merely that an Illinois-resident plaintiff interacted with the defendant’s technology in Illinois, even if that technology collects raw precursor information—such as a voice recording, photograph, or video—from which biometrics are later created. *Id.* at *2; *see also McGoveran v. Amazon Web Servs., Inc.*, No. 1:20-CV-01399-SB, 2024 WL 4626253, at *5 (D. Del. Oct. 30, 2024); *Vance v. Google LLC*, No. 20-CV-04696-BLF, 2024 WL 1141007, at *4 (N.D. Cal. Mar. 15, 2024). That is because the only conduct regulated by BIPA is the ***collection and storage of biometrics***, meaning that the statute only applies if those acts are performed in Illinois—and that cannot happen if the biometrics are created only outside of this state.

¹ Any citation herein refers to the page of the underlying document, as opposed to the ECF page.

Here, Plaintiffs allege that Defendants collected data from their devices, and then created biometric information and identifiers from that data while in cloud storage on servers hosted by an out-of-state third-party vendor, Amazon Web Services (“AWS”). Taking these allegations in the Complaint as true, Plaintiffs fail to plausibly allege that Defendants collected or stored any biometrics relating to Plaintiffs Trevor Sloan or Elmer Orpillas (“Plaintiffs”)—the only ones with a remaining BIPA claim—in Illinois. Indeed, Plaintiffs do not allege that the AWS servers on which their biometrics were created are located in this state. And judicially noticeable information confirms that they are, in fact, located elsewhere. In fact, Plaintiffs’ allegations match exactly the ones in *Compana*, *McGoveran* and *Vance*, and are insufficient to support and fail to state a claim under BIPA for the same reasons. Accordingly, Defendants move for judgment on the pleadings and ask that the Court enter judgment on Plaintiffs’ BIPA claim in Defendants’ favor.

RELEVANT FACTUAL ALLEGATIONS

Plaintiffs allege that Anker, Fantasia, and Power Mobile are, respectively, Hong Kong, Delaware, and Washington entities. Compl. ¶¶ 19–21, ECF No. 31. None is alleged to have any employees, servers, or other operations within Illinois. *See id.*

According to Plaintiffs, Defendants manufacture “eufy Security” branded security cameras, smart locks, and doorbells (collectively, “eufy Security Devices”), which they distribute and sell throughout the United States. *Id.* ¶¶ 1, 27. Defendants provide a eufy Security mobile application (“App”) that pairs with the devices, which permits users to access and personalize their devices, and view live and recorded video. *Id.* ¶ 29.

Plaintiffs claim that Defendants’ marketing “touted that the products saved all video recordings and conducted all facial recognition locally (meaning on equipment located with and controlled by the consumer).” *Id.* ¶ 2. Said otherwise, Defendants represented that their cameras

“conduct facial recognition locally, rather than transmitting [images] to cloud storage” for facial-recognition processing elsewhere. *Id.* ¶ 4. According to Plaintiffs, this “differentiate[d] [Defendants’] Camera Products from competitors’, . . . which record and process the data remotely.” *Id.* ¶ 3.

Plaintiffs claim—and they will argue—that these “statements . . . were untrue.” *Id.* ¶ 5. Specifically, Plaintiffs claim that that Defendants’ products “were uploading name-tagged thumbnail images to Anker’s AWS [Amazon Web Services]-hosted cloud storage,” where Defendants would then “use cloud-based facial recognition technology” on them. *Id.* ¶ 42; Opp’n to Mot. to Dismiss at 4, ECF No. 48. That is, Plaintiffs maintain that “images of [themselves] and others were captured by the Camera Products and thereafter transmitted and disseminated to Defendants’ cloud storage hosted by” AWS, where they were “subjected to facial recognition technology, which generated” biometric identifiers—namely, the “faceprint of individuals captured in such images.” ECF No. 31 ¶ 11; *see also id.* ¶ 124. (Plaintiffs do not allege that Defendants themselves collect anything on their own infrastructure, in Illinois or otherwise.)

These allegations, which Defendants acknowledge must be taken as true at this stage, are the crux of Plaintiffs’ BIPA claim. After all, where a biometric identifier is created and remains solely on a user’s local device, BIPA is not implicated, because the defendant does not possess, collect, or capture it. *See Barnett v. Apple Inc.*, 225 N.E.3d 602, 610–12, ¶¶ 44–45, 50–55 (Ill. 2022). Plaintiffs’ BIPA claim thus critically depends on Plaintiffs’ allegations that the creation of their biometrics occurs elsewhere—namely, in the “cloud storage hosted by” AWS. ECF No. 31 ¶¶ 11, 42.

But in circumventing one obstacle, Plaintiffs steer immediately into another—by making clear that the necessary activity to fall under BIPA (the creation of biometrics) does not take place

in Illinois. As just discussed, Plaintiffs’ theory is that instead of “conduct[ing] facial recognition *locally*,” ECF No. 31 ¶ 4, Defendants were performing “facial recognition off of [Plaintiffs’] devices,” on servers hosted by AWS. ECF No. 48 at 20. Under Plaintiffs’ theory, then, Defendants “collected, stored, used, or otherwise obtained Plaintiffs[’] . . . Biometric Data” in violation of BIPA only where those AWS cloud servers were located, because it is only there that the biometric data is even created (much less collected, stored, used, or otherwise obtained). ECF No. 31 ¶ 128. As this Court explained: “[A] ‘biometric identifier’ is not the underlying medium itself [*i.e.*, an image], . . . but instead is a set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person” that is created from that underlying medium. ECF No. 66 at 11 (citation omitted). And, according to Plaintiffs, those measurements are only created *after* the images reach the AWS cloud servers. But the Complaint does not allege that the AWS cloud infrastructure or servers at issue in this case are located in Illinois. And in fact, AWS’s publicly available—and judicially noticeable²—website confirms that those servers are located elsewhere, as *none of AWS’s cloud infrastructure or servers are located in Illinois*. See AWS, *Global Infrastructure, Regions and Availability Zones*, https://aws.amazon.com/about-aws/global-infrastructure/regions_az/ (last visited February 18, 2025). Plaintiffs’ own theory thus makes clear that the relevant acts here necessarily took place outside of Illinois.

² Courts routinely take judicial notice of AWS’s website. See *Mussat v. Power Liens, LLC*, No. 13-CV-7853, 2014 WL 3610991, at *3 (N.D. Ill. July 21, 2014) (“Courts may, at their discretion, take judicial notice of the contents of a website.”); see also *Mayhall on behalf of D.M. v. Amazon Web Servs. Inc.*, No. C21-1473-TL-MLP, 2022 WL 2718091, at *4 (W.D. Wash. May 24, 2022) (taking judicial notice of AWS’s website in BIPA action), *report and recommendation adopted*, 2023 WL 2728292 (W.D. Wash. Mar. 31, 2023); *Gladstone v. Amazon Web Servs., Inc.*, 739 F. Supp. 3d 846, 854–55 (W.D. Wash. 2024) (taking judicial notice of AWS’s website in non-BIPA action). Ultimately, though, whether the Court does the same here is beside the point, as Plaintiffs do not allege that the AWS servers at issue here are located within Illinois, which is necessary to state a claim. The AWS website simply shows why this is so—and confirms that this is not an issue that Plaintiffs could plead around through amendment.

LEGAL STANDARD

“A motion for judgment on the pleadings under Rule 12(c) of the Federal Rules of Civil Procedure is governed by the same standards as a motion to dismiss for failure to state a claim under Rule 12(b)(6).” *Adams v. City of Indianapolis*, 742 F.3d 720, 727–28 (7th Cir. 2014). A motion to dismiss under Rule 12(b)(6) challenges the sufficiency of the complaint. To survive a Rule 12(b)(6) motion, the complaint must assert a facially plausible claim and provide fair notice to the defendant of the claim’s basis. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A claim is not facially plausible unless it “pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* “[L]abels and conclusions, and a formulaic recitation of the elements” of claims will not suffice. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). While a court must take all of the well-pled factual allegations in the complaint as true, it is “not bound to accept as true a legal conclusion couched as a factual allegation.” *Id.* (citation omitted).

ARGUMENT

This Court has already held that BIPA cannot apply unless Plaintiffs allege that Defendants’ BIPA-related conduct occurred “primarily and substantially in Illinois.” ECF No. 66 at 12 (quoting *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 854 (Ill. 2005)); accord, e.g., *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *6 (N.D. Ill. Sept. 15, 2017). Indeed, the Court relied on exactly that principle to dismiss the BIPA claim as to non-Illinois resident Plaintiffs (*i.e.*, all Plaintiffs other than Sloan and Orpilla). ECF No. 66 at 12 (“agree[ing]” with Defendants’ argument that BIPA claim should be dismissed as to “non-Illinois resident Plaintiffs”). At the time Defendants filed their Motion to Dismiss, it was unclear whether a plaintiff’s residence in Illinois

was alone enough to show that a BIPA violation occurred “primarily and substantially in Illinois.” Recent caselaw now makes clear that it does not.

Specifically, a trio of recent cases hold that a BIPA claim cannot be maintained solely because plaintiffs allege that they “were ‘resident[s] and citizen[s] of the state of Illinois’” and “interacted with the Defendant’s [technology]” in this state. *Campana*, 2024 WL 2809838, at *2; *McGoveran*, 2024 WL 4626253, at *5; *Vance*, 2024 WL 1141007, at *4. That is because BIPA applies only if “the plaintiffs’ biometric information was ‘actually collected in Illinois.’” *Campana*, 2024 WL 2809838, at *2. And the mere fact that a plaintiff was “physical[ly] presen[t] in Illinois when they interacted with the defendant’s products . . . does not plausibly suggest” that the collection of biometrics “occurred ‘primarily and substantially’ in Illinois.” *Id.* at *3; *accord McGoveran*, 2024 WL 4626253, at *5 (“[B]eing from Illinois and placing a call [from which a voiceprint is created] from there is not enough to establish that the alleged conduct occurred ‘primarily and substantially’ in Illinois.”); *Vance* 2024 WL 1141007, at *4 (“[W]hile it is undisputed that Plaintiffs reside in Illinois, Plaintiffs’ residency alone is not enough . . . [to] establish[] that the alleged conduct occurred ‘primarily and substantially’ in Illinois.”).³ After all, technology can—and often does—capture only *non*-biometric information (such as audio or video recordings), which is then sent to servers elsewhere, where the biometric data is actually created by running a set of measurements on the non-biometrics source information. In those circumstances, the actual collection and storage of biometrics—the only acts regulated by BIPA—occur outside of Illinois, and so are beyond the scope of that statute.

³ Although these cases’ holdings as to the merits of BIPA are new, the principles they build on are not. Courts in this district, for instance, have long recognized that a plaintiff’s mere presence in Illinois is not sufficient to establish jurisdiction over a BIPA claim. *See, e.g., Stein v. Clarifai, Inc.*, 526 F. Supp. 3d 339, 344 (N.D. Ill. 2021).

Accordingly, a BIPA claim will not lie for an Illinois plaintiff alleging the defendant produced their voiceprint from a telephone call, unless that plaintiff also pleads facts showing that the audio data was on a server in Illinois at the time the voiceprint was created from it. *Campana*, 2024 WL 2809838, at *2; *accord McGoveran*, 2024 WL 4626253, at *5 (no BIPA claim where defendant created voice prints from audio of calls made from Illinois, because the creation of biometrics occurred on AWS “servers in Northern Virginia”). Nor can a BIPA claim be brought by a plaintiff who, in Illinois, transmits an image to a defendant, who in turn stores that image on servers outside of this state and creates biometrics from it. *Vance*, 2024 WL 1141007, at *4.

But that is all that Plaintiffs allege here—*i.e.*, that they are Illinois-residents, who interacted with Defendants’ products in this state, with the creation of biometrics occurring only elsewhere. The core of Plaintiffs’ BIPA claim is that Defendants claimed their “products saved all video recordings and conducted all facial recognition *locally* (meaning on equipment located with and controlled by the consumer),” when in fact their products were no different from their “competitors’, . . . which record and process the data remotely.” ECF No. 31 ¶¶ 2–5. Specifically, Plaintiffs maintain that Defendants’ products “were uploading name-tagged thumbnail images to Anker’s AWS-hosted cloud storage,” where Defendants would then “use cloud-based facial recognition technology” on them. *Id.* ¶¶ 4–5, 42 (alleging that Defendants’ representations that their “Products conduct facial recognition *locally*, rather than transmitting [images] to cloud storage” for remote processing, was “untrue”); ECF No. 48 at 4; *see also* ECF No. 31 ¶ 11 (“[I]mages of [Plaintiffs] and others were captured by the Camera Products and thereafter transmitted and disseminated to Defendants’ cloud storage hosted by [AWS] and subjected to facial recognition technology, which generated a face template or faceprint of individuals captured in such images.”). The location of the alleged BIPA violation—*i.e.*, where Defendants “collected,

stored, used, or otherwise obtained Plaintiffs['] . . . Biometric Data,” ECF No. 31 ¶ 128—was thus wherever the AWS-servers hosting the cloud storage were, because that is where the facial recognition data (the “Biometric Data,” *id.* ¶ 125) was created.⁴ And Plaintiffs do not (and cannot) allege that the AWS servers were in Illinois or that Defendants otherwise accessed their biometrics in Illinois in any other way. *See* ECF No. 31 ¶¶ 19–21.

Defendants thus “could not [have collected or stored biometrics] in Illinois because the servers [they] used” to allegedly create those biometrics are located outside of this state. *McGoveran*, 2024 WL 4626253, at *5. Put another way, there is not “any indication that [Defendants] did anything in Illinois,” because “Plaintiffs do not allege that [Defendants] process[], store[], or otherwise makes use of [their biometrics] in Illinois.” *Vance*, 2024 WL 1141007, at *3. In fact, the biometrics themselves never existed in this state, but were created only elsewhere (on the out-of-state AWS servers).

Accordingly, the only connection to Illinois in this case is Plaintiffs’ “physical presence in Illinois when they interacted with the [Defendants’] products.” *Campana*, 2024 WL 2809838, at *3. But Plaintiffs’ presence in Illinois is not sufficient for the Court to make a reasonable inference

⁴ While this Court previously characterized the “access to [Plaintiffs’] data without their consent” as occurring “at their residence, where they had installed the cameras,” ECF No. 66 at 12–13, Plaintiffs themselves told this Court otherwise—in both their Complaint and their Opposition to Defendants’ Motion to Dismiss. As shown above, Plaintiffs’ Complaint—from the very first page—contends that Defendants’ statements were “untrue” when they claimed that they “conducted all facial recognition [*i.e.*, the creation of biometrics] *locally* (meaning on equipment located with and controlled by the consumer),” rather than “remotely” on “servers” hosted elsewhere; meaning, in Plaintiffs’ own words, facial recognition was *not* happening “at their residence.” ECF No. 31 ¶¶ 2–5. And Plaintiffs repeated that assertion (multiple times) in their Opposition to Defendants’ Motion to Dismiss when they insisted that Defendants would conduct “facial recognition off of [Plaintiffs’] devices,” by using “cloud-based facial recognition technology” on images that had been uploaded from Plaintiffs’ devices to cloud servers elsewhere. ECF No. 48 at 4, 20. This is no accident: If Plaintiffs alleged that their biometric information had been processed or stored only locally, they could not claim a BIPA violation. *See G.T. v. Samsung Elecs. Am. Inc.*, 742 F. Supp. 3d 788, 795–97 (N.D. Ill. 2024); *Barnett*, 225 N.E.3d at 610–11.

that *Defendants'* alleged conduct occurred primarily and substantially in Illinois. *Id.* And that is especially so here, where Plaintiffs' allegations affirmatively show that the creation of biometrics occurred only elsewhere. The Court should now dismiss the BIPA claim as to all Plaintiffs, in its entirety.

CONCLUSION

For the foregoing reasons, this Court should dismiss the BIPA claim for failure to state a claim upon which relief can be granted, with prejudice.

[signatures on following page]

Dated: February 20, 2025

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Jim Houghton

Aravind Swaminathan (*Pro Hac Vice*), Lead Trial
Attorney
401 Union Street, Suite 3300
Seattle, WA 98101
P: (206) 839-4340
aswaminathan@orrick.com

Yufeng (Ethan) Ma (Ill. Bar No. 6277936)
4703 Park Place
1601 Nanjing Road West
Shanghai, 200040
People's Republic of China
P: +86 21 6109 7108
yma@orrick.com

Michael Rosenberg (Ill. Bar No. 6340654)
353 N. Clark Street, Suite 3600
Chicago, IL 60654
P. (312) 924-9833
mrosenberg@orrick.com

Jim Houghton (*Pro Hac Vice*)
222 Berkeley Street, Suite 2000
Boston, MA 02116
P: (617) 880-1800
jhoughton@orrick.com

*Counsel for Defendants Anker Innovations Limited,
Fantasia Trading LLC, and Power Mobile Life LLC*

CERTIFICATION OF SERVICE

I, the undersigned, certify that on February 20, 2025, I filed the foregoing *Memorandum of Law in Support of Motion for Judgment on the Pleadings* with the Clerk of Court using the Court's CM/ECF system, which will cause a copy of said document to be electronically transmitted to all counsel of record.

By: /s/ Jim Houghton